Combined Electronic Tax Registration
Traditional Registration System

Information for Pilot States on Testing the Exchange of XML data

I. Security Overview

The security policy for electronic data transmissions in the MTC system requires that transmissions are secure between the MTC system and each state recipient. For the purpose of this document, participating States are defined to be the client. The electronic transmission channels used for MTC-Client interactions are assumed to be secure. If the channel is not secure then the data transmission itself is assumed to be secure. In addition, the data transmission is assumed to contain the requesting client's identity credentials – a username and password. Authentication for data transmissions is performed from the client to the MTC system using a username and password combination to uniquely authenticate and identify the client to the MTC system. Client login information will be provided to the clients prior to making data transmissions available to a specific client from the MTC system.

Data transmissions will occur in one of two ways for each client. The first method is for clients to 'pull' data transmissions from the MTC system. The second method is for the MTC system to 'push' data transmissions to clients. In either case a secure electronic transmission channel for a data transmission in necessary. A client pull of a data transmission establishes this channel using the Secure Socket Layer (SSL) protocol. A push of data transmissions by MTC to clients is achieved using the File Transfer Protocol (FTP) over a secure network connection. This secure network connection is established either by using IP Security (IPsec) protocol or a Virtual Private Network (VPN) connection between MTC and the client. Any secure network will be handled at the network level and not by the application

If a data transmission is secure, but the channel/protocol used to transmit it is not, then the data transmission itself must be encrypted along with the client credentials used to access the MTC or Client systems. The method for accomplishing this for the MTC system will be to digitally sign transmissions using Public Key Infrastructure (PKI) standards commonly implemented by the use of server and client certificates. This will only be necessary if the channel cannot be secured for pushes to a state via FTP. For MTC pushes of data, this is accomplished by explicitly digitally signing the data transmission using a server certificate. In this case, the MTC system assumes the client is able to use its client certificate for decryption of the sent data transmission. The sections below provide greater detail concerning the processes just mentioned.

II. Data Transmission Options

States have two methods to choose from in order to receive taxpayer's data in XML format from the CETR system:

1. **PULL** *(Client pulls state specific data from the CETR web server)*
   a. **Web services**
   Web services are loosely coupled contracted components that communicate via XML-based interfaces. The are self contained applications that can be described, published, located, and invoked over the Internet. *The protocols used to access web services will be https and SOAP.*

   For further information go to,http://www.w3c.org/2002/ws/ or http://www.webservices.org.

   b. **Web Site download**
   MTC will host a website and provide user-id and password to clients to access the website. Once the client is authenticated they will be allowed to download the state specific XML files form the web site. After they download the file clients will acknowledge the receipt of the file. *The protocols used to allow download from a web site are https.*

2. **PUSH** *(MTC will push data to the client using ftp)*
   a. ftp (File Transfer Protocol) - A way of transferring files over the Internet from one computer to another. *The protocols used to upload a file to states site is https and ftp.*

   Data transmissions that are *pushed* from MTC to a client will occur by MTC initiating a file sent by means of FTP to the client. In order to secure the data transmission, the FTP session must be conducted over a secure network connection from MTC to the client. The FTP protocol does not inherently secure client credentials (username and password) when they are transmitted over a non-secure network connection (i.e. the Internet). For these reasons, network administration to provide for a secure channel of communication to conduct the FTP session is needed. The network protocols that allow for this type of communication are IPSec and/or Secure VPN network connections as previously mentioned in the document.

Examples of the above two data transmission methods are provided in Section IV

III. Information required by State and MTC to Configure the transmission of data

States are allowed to select one method of data transmission either push or pull.

For states that have chosen to PULL information the following information will be provided:

- States that have chosen Web Service method
  - The name and address of the web service
  - The client will have to build their SOAP client to access the web services
- States that have chosen to use download files from CETR website
  - MTC will provide a user id and password to state representative
  - MTC will provide a URL to log on to the web site
  - Upon logging and validation state will be able to access their own state specific XML files

For states that have chosen to PUSH information the following information needs to be provided to MTC:

- States will provide ftp logon information to MTC
- States will provide user id and password to access the ftp site
- States will provide a time when the upload of XML file will take place

IV. Examples of Data Transmission to a Client

Client *Pulls* Data from the MTC System

Data transmissions that are p*ulled* from MTC will occur by a client initiating a file download by one of two means: Web Site Download or Web Service.

Web Site Download (Protocols: SSL / HTTPS)

1. The MTC System will setup a web site that can only be accessed via HTTPS (i.e. – https://<mtc_web_site>/<download_page>).
2. This web site will prompt all visitors for their client logins via a web form login.
3. After the client logs into the web site successfully, the client will be presented with available data transmission(s) to download.
4. The client will click the appropriate link for the tax payer data file and proceed to complete the download.
5. After successful completion of the download, the client will proceed to an acknowledgement page to deliberately acknowledge receipt of the electronic data transmission. Acknowledgement will be dependant on a unique string identifier sent inside the data transmission. This identifier must be provided to the MTC system at the time of acknowledgement.

Web Service (Protocols: HTTPS / SOAP)

1. The client will be given the URL of an available web service for use (i.e. – https://<mtc_web_site>/<web_service>)
2. The client will develop programmatic functionality to call the *web methods* exposed by this web service.
3. The client will need to provide their user id and password (provided by MTC) in order to access the following methods.
4. The client will call the first method, "getDocument()", to receive a data transmission.
5. After completion of the data transmission the client will call the second method, "acknowledgeDocument(String strAckID)", to acknowledge the data transmission it just received.

A Microsoft .NET example of steps(2- 4) is illustrated below.

In an existing .NET project using Microsoft Visual Studio .NET 2003 perform the following steps:

1. From the main menu click menu selections **Project** > **Add Web Reference**.
2. In the **URL:** text box type the address for the web service. For example: **https://www.mtc.com/DataTransmissions.asmx .**
3. After the web service has been found successfully, click the **Add Reference** button. (Note: Be sure to make remember the value in the **Web reference name:** text box above this button.)

4. Inside a method of executable code for this project type the **Web reference name:** value and a period. The 'Intelli-sense' feature of Microsoft Visual Studio should show the name of the web service proxy used to communicate to the web service.
5. Declare a local variable using this type (proxy object).
6. Call the "getDocument()", and "acknowledgeDocument(String strAckID)" methods of this object. Where 'strAckID' is set to the unique identifier provided in the data transmission sent.

MTC System *Pushes* Data to the Client

Data transmissions that are *pushed* from MTC to a client will occur by MTC initiating a file sent by means of FTP to the client. In order to secure the data transmission, the FTP session must be conducted over a secure network connection from MTC to the client. The FTP protocol does not inherently secure client credentials (username and password) when they are transmitted over a non-secure network connection (i.e. the Internet). For these reasons, network administration to provide for a secure channel of communication to conduct the FTP session is needed. The network protocols that allow for this type of communication are IPSec and/or Secure VPN network connections as previously mentioned in the document.

Automated FTP (Protocols: FTP - transmitted over IPSec or VPN)

1. The client will setup an FTP account accessible over a secure network connection.
2. The client will give the MTC the username and password for this account.
3. MTC will automatically access the client via FTP using the secure network connection daily on a schedule designated by the client.
4. MTC will send the data transmission to the client and disconnect from the client after transmission.
5. The client, after receiving the data transmission will navigate to a MTC system web site, and successfully login using a username and password.
6. The client will be shown an acknowledge web page by which they can enter the acknowledgement of the data transmission using a unique identifier supplied inside the data transmission.